

## Addressing Security Concerns in Virtual Environments

**Christofer Hoff**

**Chief Architect, Security Innovation**

**Unisys**

**February 4, 2008**

# VIRTUALIZATION

**chicken little**



# Talking Points

- Virtualization: Floor Wax & Dessert Topping
- Woot! Virtualization Rocks!
- Mama says “Virtualization is da Devil!”
- Today’s Risk Model is Kaput!
- Threats, Vulnerabilities & Hype
- Pragmatism & Perspective: Taking Action Today
- The Quest for the Holy Grail
- I’m OK, You’re OK.





# Virtualization: Floor Wax & Dessert Topping

- Virtualization is often technically defined as:

“

...an abstraction layer that decouples the physical hardware from the operating system to deliver greater resource utilization and flexibility

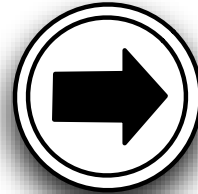
”

- But it's really about two things:
  - Time
  - Money



# Virtualization Is About More Than Just Servers

- Servers
- Clients
- Networks
- Storage
- Operating Systems
- Applications
- Security
- Access
- Information
- Operations



Resources

- Partitioning
- Isolation
- Encapsulation

Platforms

# w00t! Virtualization Rocks!

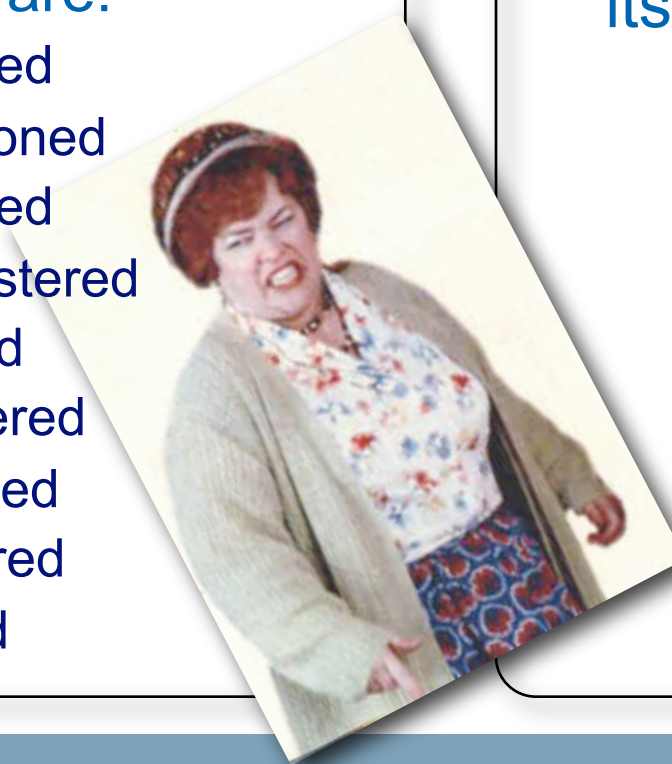
- 
- Physical Consolidation
  - Cost Reduction
  - Ease and flexibility of Provisioning
  - On-demand Resource Pooling
  - Disaster Recovery
  - Capacity on-Demand
  - Application Availability
  - Management of Service Levels

- Easy Backup
- Fault Tolerance
- Eases Application Lifecycle Management
- Provides Development Efficiencies
- Allows for ubiquitous Computing
- Application Portability
- Secure computing environments...

# Mama Says “Virtualization Is Da Devil!”

- Virtualization changes the way resources & networks are:

- Designed
- Provisioned
- Deployed
- Administered
- Patched
- Recovered
- Assessed
- Monitored
- Audited



- ...and how information across its lifecycle is:

- Created
- Stored
- Controlled
- Accessed
- Destroyed
- Archived, and
- **Secured**

# Highly Scientific Poll #1

## What Fraction of Your Servers Are Virtualized?

- a. 0%
- b. 1%-25%
- c. 26%-50%
- d. 51% to 75%
- e. 76% to 99%
- f. 100%

*Source: Information Week 2007 Analytics Brief : Securing the New Data Center*



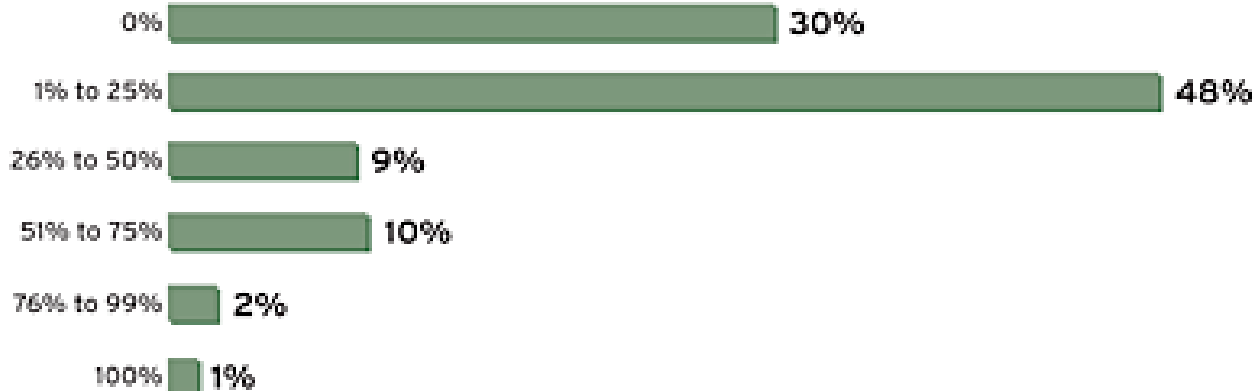
# Survey Says!

---

## VM Volume

---

What fraction of your servers are virtualized?



Source: InformationWeek Poll

# Highly Scientific Poll #2

**Does your organization have a formal security/information protection strategy for virtualization server environments**

- a. No IT Security/protection in place for virtual servers
- b. A VM-tailored strategy and solution is in place
- c. VM servers comply with company standards defined by conventional server infosec policy
- d. We're working on it!

*Source: Information Week 2007 Analytics Brief : Securing the New Data Center*

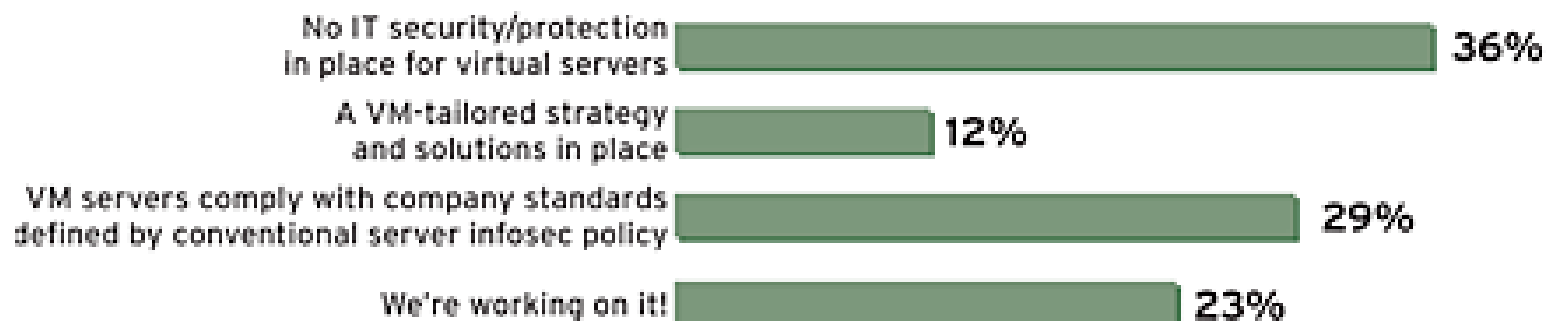
# Survey Says!

---

## Security Strategy

---

Does your organization have a formal security/information protection strategy for virtualization server environments?



---

Source: InformationWeek Poll

# Whoops!

## The Phantom Menace: Unmanaged VMs and VM “Appliances”

**By 2010, unmanaged VMs will be as significant an issue to enterprises as unmanaged devices are in 2007 (0.9 probability).**

**“Best Practices and Security Considerations for Securing Virtual Machines” G00144828 March 2007**

**Gartner.**

# Highly Scientific Poll #3

## How do virtual servers compare with conventional server environments for information protection and security

- a. VMs are as secure and safe as conventional servers
- b. VMs are more prone to risk than conventional servers
- c. VMs are less prone to risk than conventional servers

*Source: Information Week 2007 Analytics Brief : Securing the New Data Center*

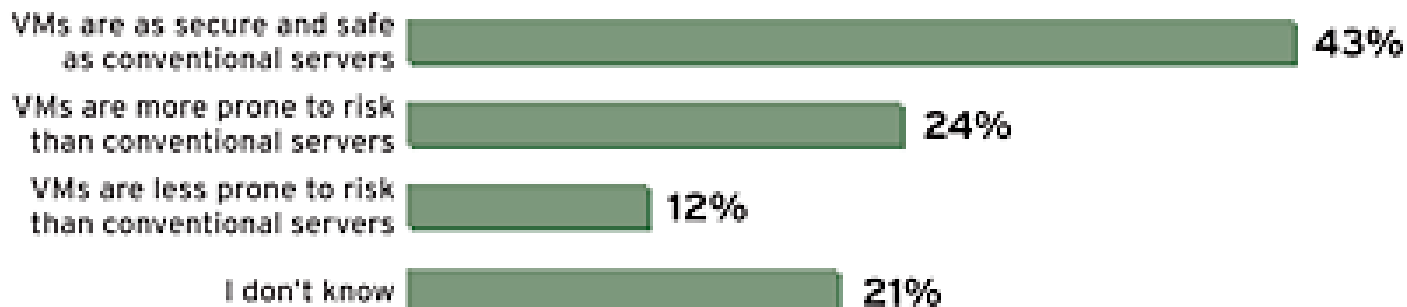
# Survey Says!

---

## Confidence Level

---

In your opinion, how do virtual servers compare with conventional server environments for information protection and security?



---

Source: InformationWeek Poll

# We Have a Failure To Communicate!

## **Most Virtual Machines Deployed Will Be Less Secure than Their Physical Counterparts**

**Through 2009, 60% of production Virtual Machines will be less secure than their physical counterparts (0.8 probability).**

**“Best Practices and Security Considerations for Securing Virtual Machines” G00144828 March 2007**

**Gartner.**

# Today's Risk Model is Kaput!

- Virtualization takes every issue we have today in security and amplifies them
- Crunchy on the outside and even more gooey in the middle! One moat, lots of castles
- Increased operational risk; SoD, role change, loss of visibility
- Unprepared for new attack surfaces and threat vectors
- Immature management and security solutions
- Transitive technology mated to static controls & approaches to security





# How Do We Assess Risk in a Virtualized Environment?

## Burton Group's 5 Immutable (?) Laws of Virtualization

**Law 1:** Attacks against the OS and applications of a physical system have the exact same damage potential against a duplicate virtual system.

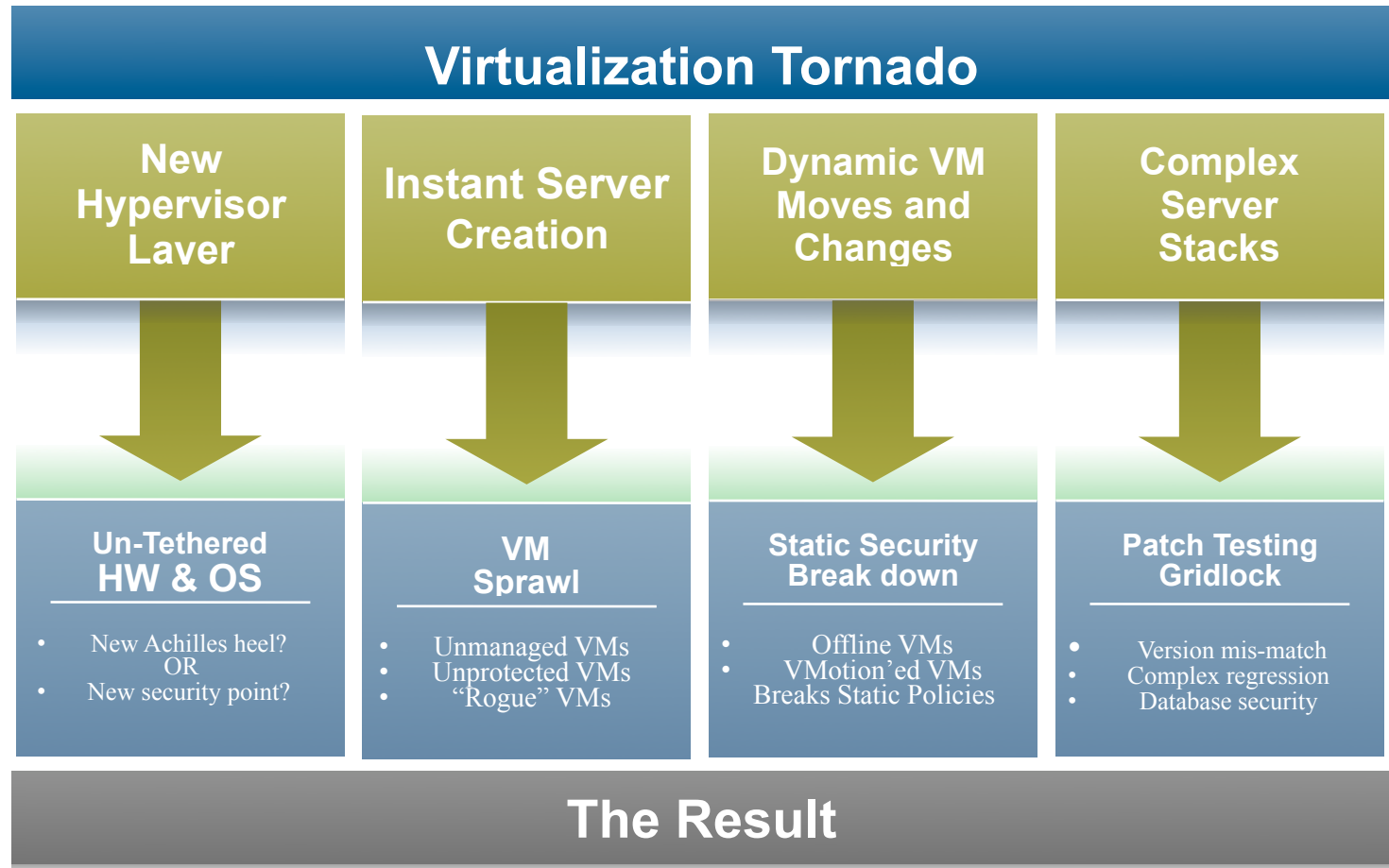
**Law 2:** A VM has higher risk than its counterpart physical system that is running the exact same OS and applications and is configured identically.

**Law 3:** VMs can be more secure than related physical systems providing the same functional service to an organization when they separate functionality and content that are combined on a physical system.

**Law 4:** A set of VMs aggregated on the same physical system can only be made more secure than its physical, separate counterparts by modifying the configurations of the VMs to offset the increased risk introduced by the hypervisor.

**Law 5:** A system containing a “trusted” VM on an “untrusted” host has a higher risk level than a system containing a “trusted” host with an “untrusted” VM.

# Virtualization Makes Simplicity Complex?



Slide Courtesy of:  BlueLane™

# Hypervisors = Disruptive Commodity?

**Seems everybody's got one...**

- ▶ VMware
- ▶ Citrix
- ▶ Microsoft
- ▶ Oracle
- ▶ Phoenix

**...and they're showing up in all sorts of places**

- ▶ Servers
- ▶ Clients
- ▶ Appliances
- ▶ Mobile Platforms (?)

# The Battle for the Datacenter OS

- Upgrading from servers to blades
- Moving from hosts and switches to clusters and fabrics
- Evolving from hardware/software affinity to grid/utility computing
- Transitioning from infrastructure to service layers in “the cloud”



*“A hundred years ago, companies stopped producing their own power with steam engines and generators and plugged into the newly built electric grid.” - Nicholas Carr, the Big Switch*

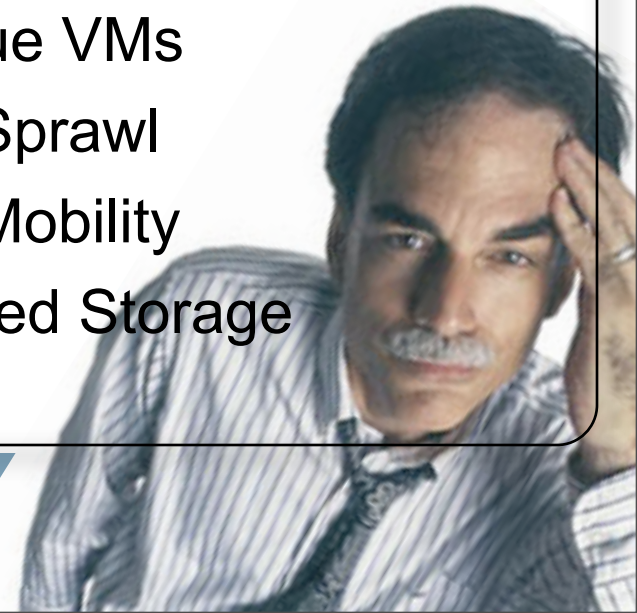
# Some Things To Worry About Today

## ■ Operational Risks

- Immature Mgmt & Security Tools
- Virtual networking misconfiguration
- Transition & separation of duties
- Vulnerability Mgmt Lifecycle (on/offline VM)
- Inconsistent Security Policies/Procedures
- Loss of IDP Visibility

## ■ Threats & Vectors

- Guest-hopping (Intra-VM) attacks
- Vulnerabilities in HV
- Attack management stacks
- Theft of an intact VM
- Rogue VMs
- VM Sprawl
- VM Mobility
- Shared Storage



# Some Things To Worry About Later

- Things you can't do much about today but are important to think about:
  - Hypervisor subversion (Hyperjacking)
  - Virtualization-aware malware
  - Virtualization Chipset malware
  - Adding to the OS Monoculture
  - Thinner hypervisors yet exposing more dense functionality via API
  - Moore's Law (multicore) Crisis\*



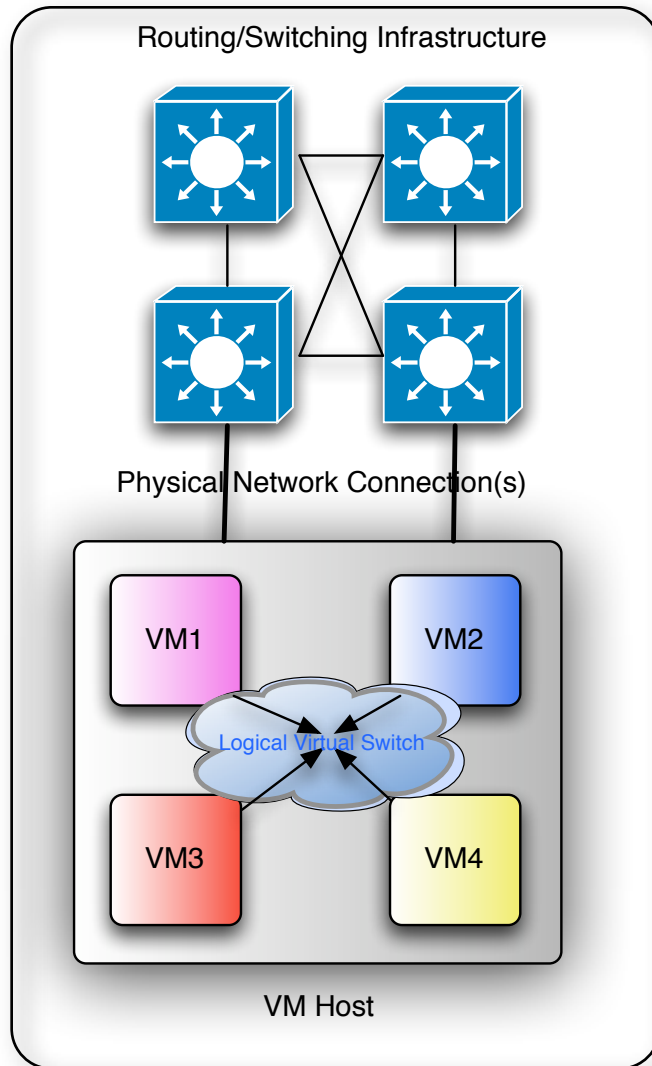
[\\*http://smoothspan.wordpress.com/2007/09/06/a-picture-of-the-multicore-crisis/](http://smoothspan.wordpress.com/2007/09/06/a-picture-of-the-multicore-crisis/)

# Securing Virtualized Environments

- Examine our options today
- See what's expected in the near term
- Paint a picture of what we'd like to see in the long term
- Provide some pragmatic advice
- Offer some examples



# The Network is the Computer...



- Let's say that we have a single physical host which is connected to the physical switched network via Gb/s Ethernet
- Further, we have 4 VM's in a that single physical host each representing components of an application stack
- The bulk of communications are between the the VM's utilizing intra-VM communications across the virtual switch fabric and does not touch the physical network
- Thus, the network *is* the computer or vice versa?
- **How does the “network” supposedly self-defend when it's not even used?**



# Secure the Networks Hosting the VM Today...Common Sense Stuff

## ■ Options:

- Segment your network based on criticality, function or access
- Deploy embedded security across the network infrastructure
- Deploy Security as a best-of-breed overlay Virtualized Service Layer
- Evolve along the virtualization security model continuum we're about to discuss
- Integrate Host & Network Protection Schemes and tie in telemetry
- Monitor, monitor, monitor
- **All of the above**

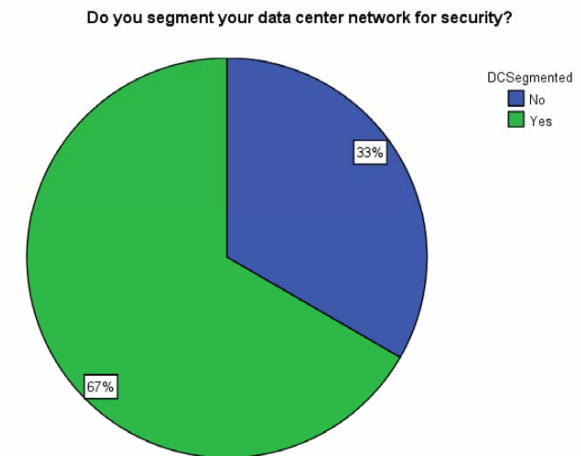
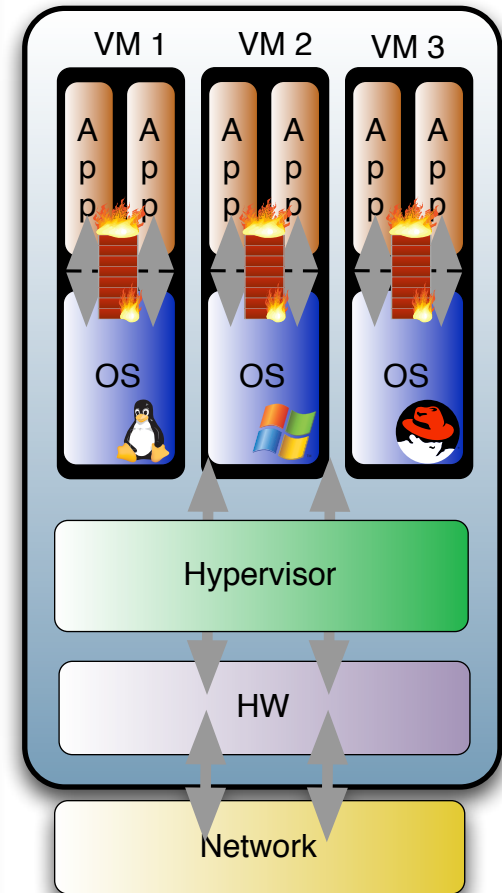


Figure 3: Data Center Security Segmentation



# Security Software in the VM

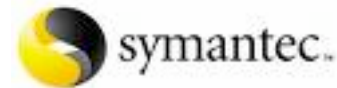
- Security Software installed on each VM
- Protects only that VM
- Limited visibility
- Unaware that the VM is virtualized
- Same management functionality as today
- Does not reduce costs



You Can Do This Now

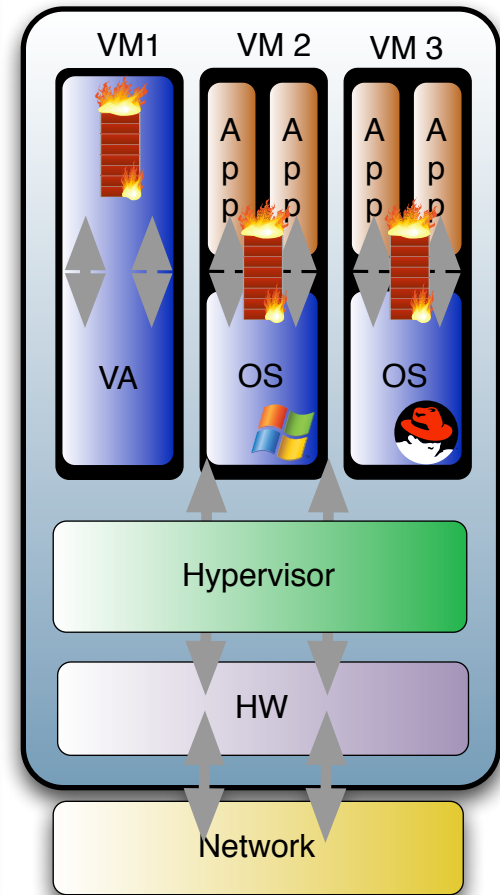
# Today: The Usual Suspects...

- Most anything you run today in your conventional environments will work here...
  - Firewalls
  - HIDS
  - HIPS
  - Anti-virus
  - NAC
  - Endpoint Assurance
  - Patch Management
  - Configuration Audit & Control
  - ...

The McAfee logo, featuring the word "McAfee" in a bold, red, sans-serif font with a registered trademark symbol.The Check Point logo, consisting of a small icon of a computer monitor with a checkmark, followed by the text "Check Point" and "SOFTWARE TECHNOLOGIES LTD." in a smaller font, and the tagline "We Secure the Internet." below it.The Cisco logo, featuring a stylized bridge icon above the word "CISCO" in a bold, red, sans-serif font.The Tripwire logo, featuring the word "tripwire" in a white, lowercase, sans-serif font inside an orange rounded rectangle.The QnetIQ logo, featuring a stylized "Q" icon made of three colored squares (yellow, green, blue) followed by the text "netIQ" in a bold, black, sans-serif font.The Symantec logo, featuring a stylized "S" icon made of two overlapping circles (yellow and black) followed by the word "symantec." in a lowercase, black, sans-serif font.The ConfigureSoft logo, featuring the word "Configuresoft" in a blue, lowercase, sans-serif font.The Trend Micro logo, featuring a stylized "T" icon inside a red circle followed by the text "TREND MICRO" in a bold, black, sans-serif font.The BigFix logo, featuring a stylized "B" icon made of two overlapping circles (blue and green) followed by the text "BIGFIX" in a bold, black, sans-serif font.

# Virtualized IDP as Virtual Appliance/VM

- Security software installed in a VM as a virtual appliance
- Paired with software installed in VMs per previous model
- Allows virtualization of security across Host
- Requires virtual networking configuration
- Better Intra-VM visibility

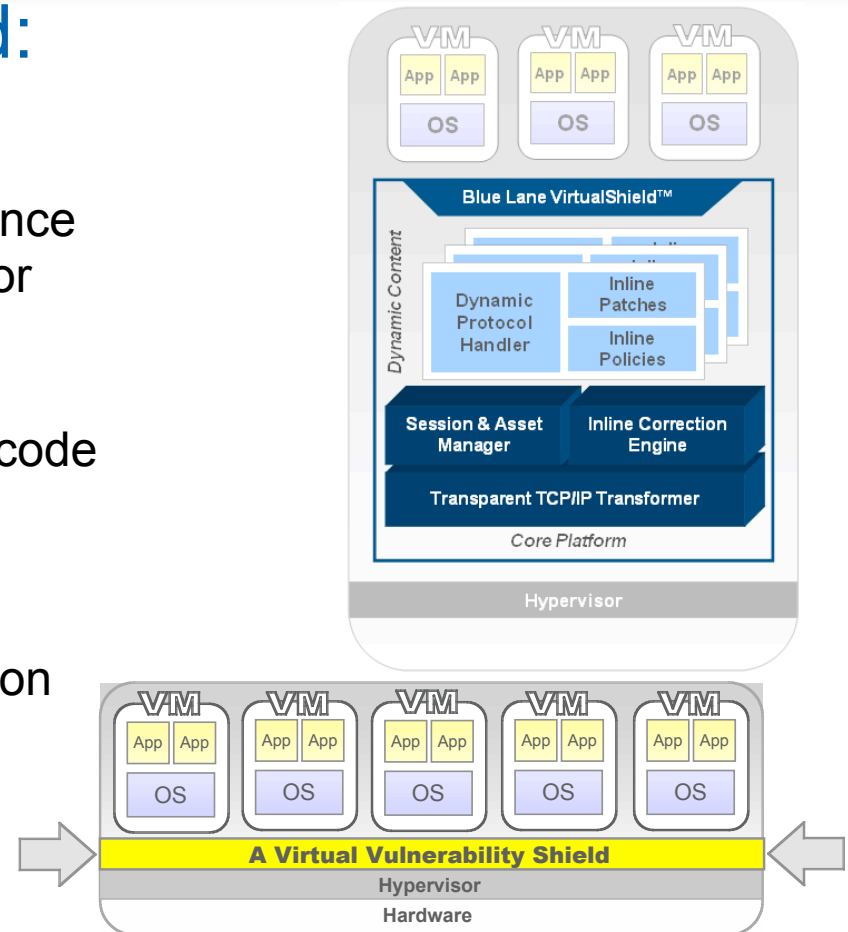


You Can Do This Now

# Today: BlueLane's VirtualShield

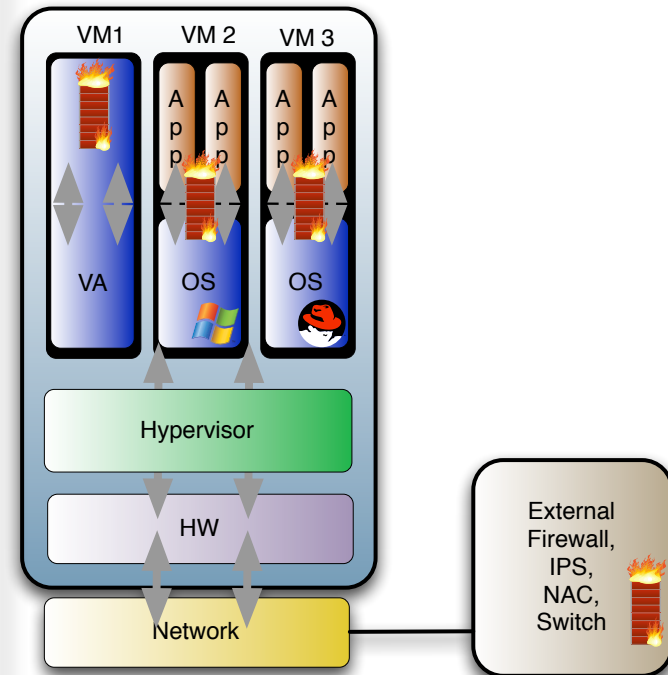
## ■ BlueLane's VirtualShield:

- Purpose-built virtual appliance
  - No hardware assist required
  - Zero packet copies through appliance
  - Tight integration with the hypervisor
- High-performance core platform
  - High throughput, low latency
  - Full session context & protocol decode
  - Integrated with Virtual Center
- Dynamically loadable content
  - Breadth of coverage options
  - On-demand assignment & execution
- Security function consolidation
  - Vulnerability detection/correction
  - App & server-specific policies
  - User, usage-based access control



# Virtualized IDP Interacting with Security Fabric

- Same as previous model but adds interaction with external security devices
- Better performance
- Ability to tie into non-virtualized security fabric
- Ability to apply same policies across physical/virtual

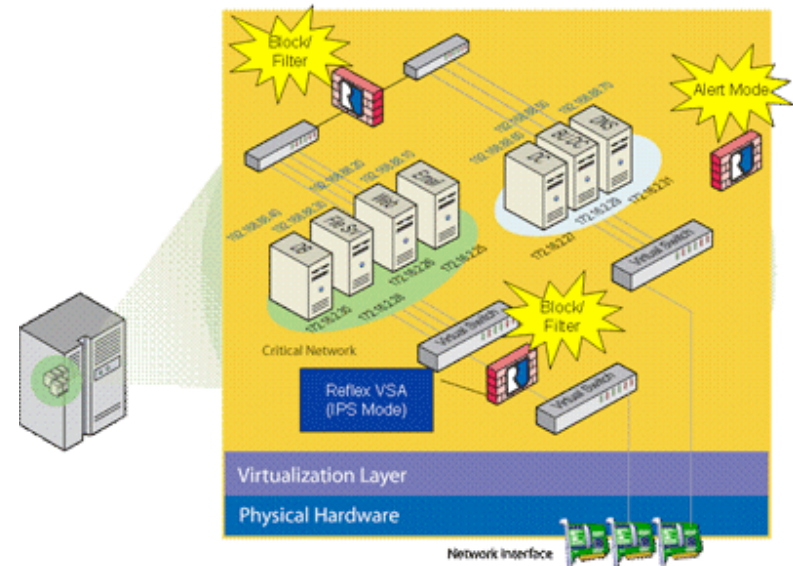


You Can Do This Now

# Today: Reflex VSA

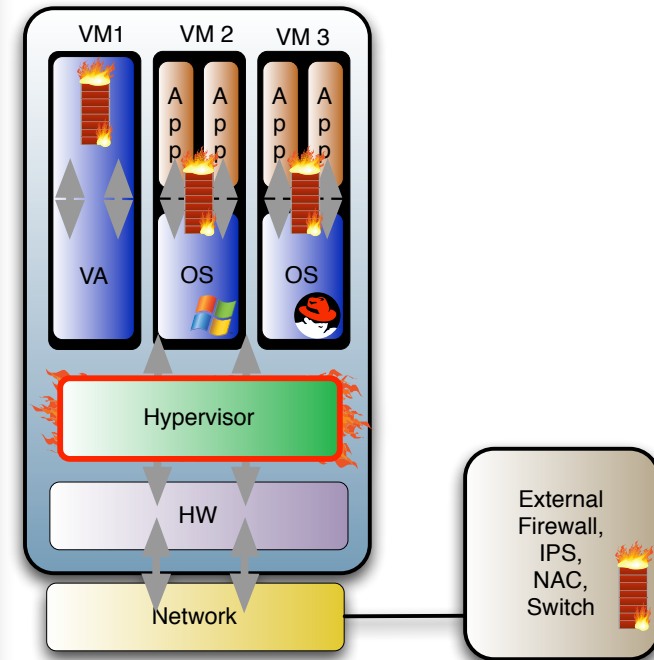
## ■ Reflex VSA

- Access firewall for permission enforcement for intra-VM and external network communication
- Intrusion Prevention with inline blocking and filtering for virtualized networks
- Anomaly, signature, and rate-based threat detection capability
- Network Discovery to discover and map all virtual machines and applications
- Centralized configuration and management console, comprehensive reporting tools, and real-time event aggregation and correlation
- Works in conjunction with physical security switches



# ...adding Security in the Hypervisor

- Same as previous model but adds/relies upon additional security capabilities in the hypervisor
- Tighter integration between third party security functions, HV and management toolsets

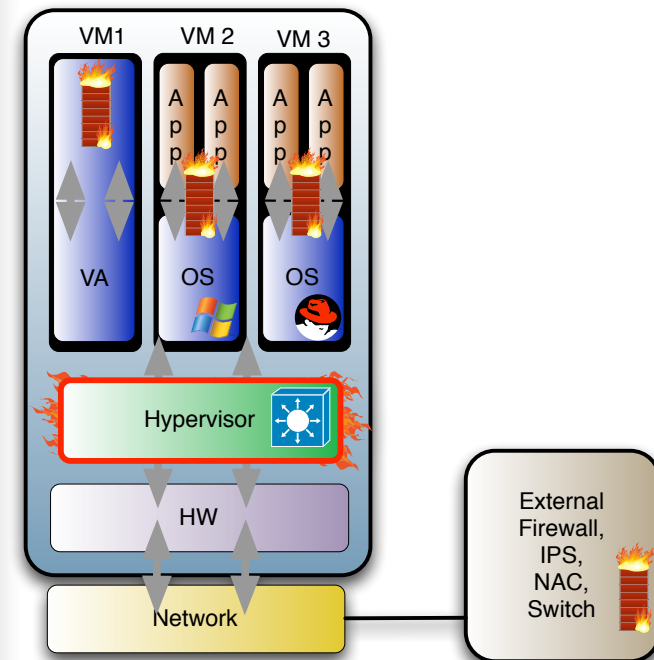


Coming Soon...



# ...With Third Party Virtual Switches

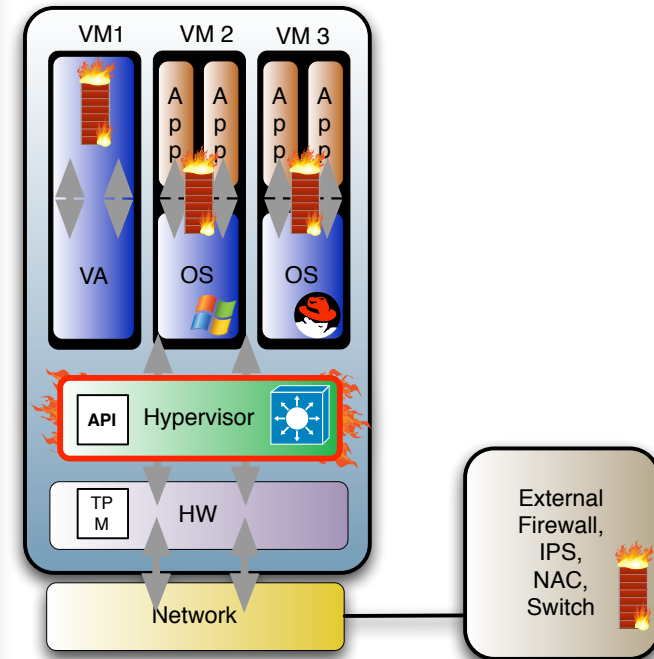
- Same as previous model but now allows for choice of vSwitches
- Allows integration/replication of external software, fabric capabilities and policy
- Enhanced Security
- Enhanced Flexibility



Bueller?...

# ...With TPM and Exposure of HV APIs

- Same as previous model but now exposes native HV functionality via APIs
- Integrates TPM for trust model, assurance & extension of functionality
- Allows the HV to become thinner
- Defines the Security Subsystem



Santa? Easter Bunny?

# I'm OK, You're OK - Things We Can Do Today

- Follow your virtualization environment provider's and industry guidelines for security.
- Apply at least the same strategies to your VM's that you use for your non VM environments
- Segment your network; isolate by function, criticality and security
- Treat each VM Host as a perimeterized DMZ
- Monitor and extract really good telemetry and instrumentation
- Baseline your network NOW before something bad happens
- Explore New Technologies such as Blue Lane, Reflex
- Virtualize Security Service Layers across network infrastructure
- Enforce rigorous control over admins with auditing and device management (physical and logical)
- Push our vendors to develop solutions for virtualized environments



# The Quest For the Virtualization Security Holy Grail

1. We need affinity between the VM and protection schemes; security policy moves with the VM
2. Centralized VM registration providing physical Hardware/VM Registration Services that controls VM spin-up (TPM)
3. Comprehensive discovery, profiling, & dynamic protection of all VM's
4. Integrated Network Admission Control & Network Access Control for VMs at the Virtual Switch layer
5. Implement a trust model in hardware & software
6. Behavioral Anomaly Detection (network & content)
7. Rootkit Detection for both hardware and software layers
8. Correlation of telemetry between VM Management and security planes
9. Separate and secure control/data paths
10. Tie in network security functions, host controls and VM/Hypervisor provisioning & defenses into a consolidated single pane of glass for virtualized management (think Cisco's vFrame)



# Summary Advice for InfoSec Types

- Don't hate the player, hate the game!  
Virtualization is unavoidable, don't try...you will be assimilated
- Virtualization is a useful thing; your CIO wants it. You should, too.
- If you're security sucks now, you'll be comforted by the lack of change when you deploy virtualization!
- Use the opportunity to bring your developers, the network, security teams and the auditors closer...even if blunt-force trauma ensues
- There's no silver bullet, but a lot of silver buckshot...use it all



# Questions/Comments?

Christofer Hoff

Chief Architect, Security Innovation - Unisys

[Christofer.Hoff@Unisys.com](mailto:Christofer.Hoff@Unisys.com)

+1.978.631.0302

Blog:

<http://rationalsecurity.typepad.com>

